TUGAS UJIAN TENGAH SEMESTER

KEAMANAN JARINGAN KOMPUTER

Muhammad Zikrillah

09121001050

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016

SCANNING dan CVE

Domain Name Target: www.ceritakecil.com

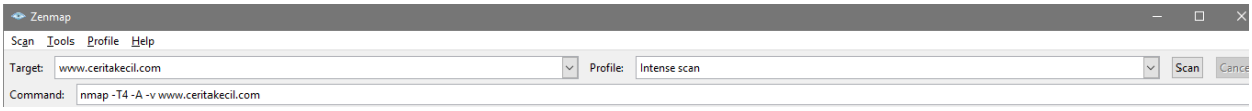
Percobaan kali ini menggunakan scanner tools untuk mencari informasi lebih lanjut dari sebuah target dengan cara menscanning target tersebut. Adapun informasi yang akan dicari dari target tersebut yaitu mengenai open port, daemon, vulnerability, serta cve yang akan dijadikan cve mapping.

Adapun scanner tools yang akan digunakan adalah sebagai berikut:

- Nmap (Zenmap)
- Nessus
- Port Scanner

1. Nmap (Zenmap)

Pada percobaan pertama menggunakan scanning tools Nmap (Zenmap) yang didapat dari website www.nmap.org/zenmap. Dari zenmap tersebut kita masukan nama domain target kita www.ceritakecil.com dengan profile intense scan, kemudian kita scan.



Berikut hasil scanning yang hanya di screenshot pada bagian informasi yang ingin kita cari:

A. Open Port

```
Starting Nmap 7.11 ( https://nmap.org ) at 2016-03-27 11:29 SE Asia Standard Time
NSE: Loaded 138 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:29
Completed NSE at 11:29, 0.00s elapsed
Initiating NSE at 11:29
Completed NSE at 11:29, 0.00s elapsed
Initiating Ping Scan at 11:29
Scanning www.ceritakecil.com (74.220.215.246) [4 ports]
Completed Ping Scan at 11:29, 1.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:29
Completed Parallel DNS resolution of 1 host. at 11:30, 13.00s elapsed
Initiating SYN Stealth Scan at 11:30
Scanning www.ceritakecil.com (74.220.215.246) [1000 ports]
Discovered open port 53/tcp on 74.220.215.246
Discovered open port 110/tcp on 74.220.215.246
Discovered open port 8080/tcp on 74.220.215.246
Discovered open port 143/tcp on 74.220.215.246
Discovered open port 995/tcp on 74.220.215.246
Discovered open port 80/tcp on 74.220.215.246
Discovered open port 21/tcp on 74.220.215.246
Discovered open port 25/tcp on 74.220.215.246
Discovered open port 22/tcp on 74.220.215.246
Discovered open port 587/tcp on 74.220.215.246
Discovered open port 443/tcp on 74.220.215.246
Discovered open port 993/tcp on 74.220.215.246
Discovered open port 26/tcp on 74.220.215.246
Discovered open port 465/tcp on 74.220.215.246
Completed SYN Stealth Scan at 11:30, 17.79s elapsed (1000 total ports)
Initiating Service scan at 11:30
Scanning 14 services on www.ceritakecil.com (74.220.215.246)
Completed Service scan at 11:32, 143.45s elapsed (14 services on 1 host)
```

Dari data diatas domain name www.ceritakecil.com dengan ip 74.220.215.246 memiliki 14 open port sebagai berikut:

No.	Open Port	Protocol
1	53	Tcp
2	110	Tcp
3	8080	Tcp
4	143	Tcp
5	995	Tcp
6	80	Tcp
7	21	Tcp
8	25	Tcp
9	22	Tcp
10	587	Tcp
11	443	Tcp
12	993	Tcp
13	26	Tcp
14	465	Tcp

B. Daemon (Service)

Daemon merupakan sebuah proses yang bekerja pada background karena proses ini tidak memiliki terminal pengontrol. Dalam sistem operasi Windows biasanya lebih dikenal dengan sebutan service.

```
PORT     STATE  SERVICE  VERSION
21/tcp   open   ftp      Pure-FTPd
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
22/tcp   open   ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 f2:f8:96:d0:c9:34:f2:16:f1:5b:c3:21:cf:b9:5d:4d (DSA)
|_  1024 be:ae:7d:3b:81:fc:3f:3a:67:49:a3:56:24:69:b8:09 (RSA)
25/tcp   open   smtp
|_smtp-commands: [74.220.215.246] Hello [192.168.130.242], pleased to meet you, ENHANCEDSTATUSCODES, PIPELINING, 8BITMIME, SIZE 10485760, DSN, AUTH LOGIN PLAIN,
DELIVERBY, HELP,
26/tcp   open   smtp     Exim smtpd 4.86_2
| smtp-commands: host246.hostmonster.com Hello www.ceritakecil.com [114.125.44.77], SIZE 52428800, 8BITMIME, AUTH PLAIN LOGIN, STARTTLS, HELP,
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
|_ssl-date: 2016-03-27T04:33:30+00:00; +2s from scanner time.
53/tcp   open   domain?
80/tcp   open   http     Apache httpd
|_http-favicon: Unknown favicon MD5: 3C5F44ACD9E8664F5AA74215398F4940
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 10 disallowed entries
| /admin/ /css/ /extra/ /flash/ /fonts/ /images/ /include/
|_/library/ /scripts/ /tagCloud/
|_http-server-header: nginx/1.8.1
|_http-title: Cerita pendek anak-anak, dongeng, ilmu pengetahuan umum, tokoh...
110/tcp  open   pop3     Dovecot pop3d
|_pop3-capabilities: CAPA SASL(PLAIN LOGIN) USER AUTH-RESP-CODE TOP UIDL STLS RESP-CODES PIPELINING
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2016-03-27T04:33:25+00:00; +1s from scanner time.
113/tcp  closed ident
143/tcp  open   imap     Dovecot imapd
|_imap-capabilities: listed LOGIN-REFERRALS SASL-IR IMAP4rev1 more ID IDLE post-login OK LITERAL+ capabilities Pre-login AUTH=LOGINA0001 AUTH=PLAIN have ENABLE
STARTTLS
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2016-03-27T04:33:34+00:00; +2s from scanner time.
443/tcp  open   ssl/http Apache httpd
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Apache
```

```
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2016-03-27T04:33:24+00:00; +2s from scanner time.
465/tcp  open   ssl/smtp Exim smtpd 4.86_2
|_smtp-commands: host246.hostmonster.com Hello www.ceritakecil.com [114.125.44.77], SIZE 52428800, 8BITMIME, AUTH PLAIN LOGIN, HELP,
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2016-03-27T04:33:34+00:00; +2s from scanner time.
587/tcp  open   smtp     Exim smtpd 4.86_2
| smtp-commands: host246.hostmonster.com Hello www.ceritakecil.com [114.125.44.77], SIZE 52428800, 8BITMIME, AUTH PLAIN LOGIN, STARTTLS, HELP,
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2016-03-27T04:33:24+00:00; +2s from scanner time.
993/tcp  open   ssl/imap Dovecot imapd
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2016-03-27T04:33:24+00:00; +2s from scanner time.
995/tcp  open   ssl/pop3 Dovecot pop3d
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2016-03-27T04:33:24+00:00; +2s from scanner time.
1723/tcp closed pptp
8080/tcp open   http     Apache httpd
|_http-favicon: Unknown favicon MD5: 3C5F44ACD9E8664F5AA74215398F4940
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 10 disallowed entries
| /admin/ /css/ /extra/ /flash/ /fonts/ /images/ /include/
|_/library/ /scripts/ /tagCloud/
|_http-server-header: nginx/1.8.1
```

Dari data diatas dapat diinformasikan sebagai berikut:

No.	Open Port	Protocol	Service (Daemon)	Version
1	21	Tcp	ftp	Pure-Ftpd
2	22	Tcp	Ssh	Open ssh 5.3 (Protocol 2.0)
3	25	Tcp	Smtp	
4	26	Tcp	Smtp	Exim smtpd 4.86_2
5	53	Tcp	Domain	
6	80	Tcp	http	Apache httpd
7	110	Tcp	Pop3	Dovecot Pop3d
8	143	Tcp	Imap	Dovecot imapd
9	443	Tcp	Ssl/http	Apache Httpd
10	465	Tcp	Ssl/smtp	Exim smptd 4.86_2
11	587	Tcp	Smtp	Exim smptd 4.86_2
12	993	Tcp	Ssl/imap	Dovecot imapd
13	995	Tcp	Ssl/pop3	Dovecot Pop3d
14	8080	Tcp	http	Apache Httpd

Untuk aplikasi scanning tools zenmap tidak dapat ditemukan vulnerability maupun cve nya.

2. Nessus

Pada percobaan kedua kita menggunakan scanning tools Nessus yang didapat dari website www.nessus.org. Dari nesssus tersebut kita harus login terlebih dahulu;

Kemudian pada scan library kita pilih Basic Network Scan, lalu kita masukkan perintah yang ada disana dan masukkan juga target yang akan kita cari informasinya.

Berikut merupakan hasil scanning yang hanya di screenshot pada bagian informasi yang ingin kita cari:

A. Open Port

Output

```
Port 21/tcp was found to be open
```

Port	Hosts
21 / tcp / ftp	www.ceritakecil.com

```
Port 22/tcp was found to be open
```

Port	Hosts
22 / tcp / ssh	www.ceritakecil.com

```
Port 25/tcp was found to be open
```

Port	Hosts
25 / tcp / smtp	www.ceritakecil.com

```
Port 53/tcp was found to be open
```

Port	Hosts
53 / tcp	www.ceritakecil.com

```
Port 80/tcp was found to be open
```

Port	Hosts
80 / tcp / www	www.ceritakecil.com

```
Port 110/tcp was found to be open
```

Port	Hosts
110 / tcp / pop3	www.ceritakecil.com

```
Port 143/tcp was found to be open
```

Port	Hosts
143 / tcp / imap	www.ceritakecil.com

```
Port 443/tcp was found to be open
```

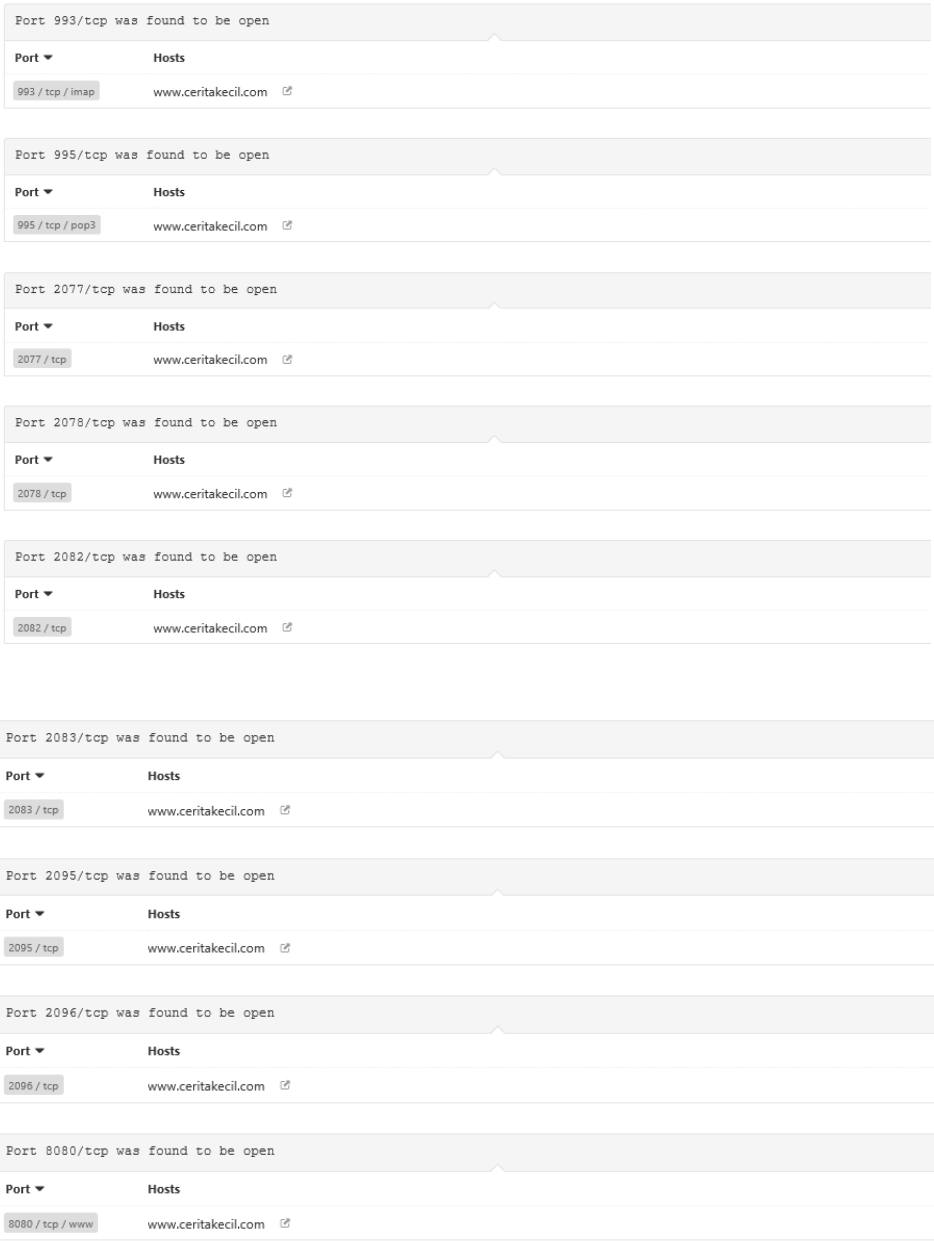
Port	Hosts
443 / tcp / www	www.ceritakecil.com

```
Port 465/tcp was found to be open
```

Port	Hosts
465 / tcp / smtp	www.ceritakecil.com

```
Port 587/tcp was found to be open
```

Port	Hosts
587 / tcp / smtp	www.ceritakecil.com

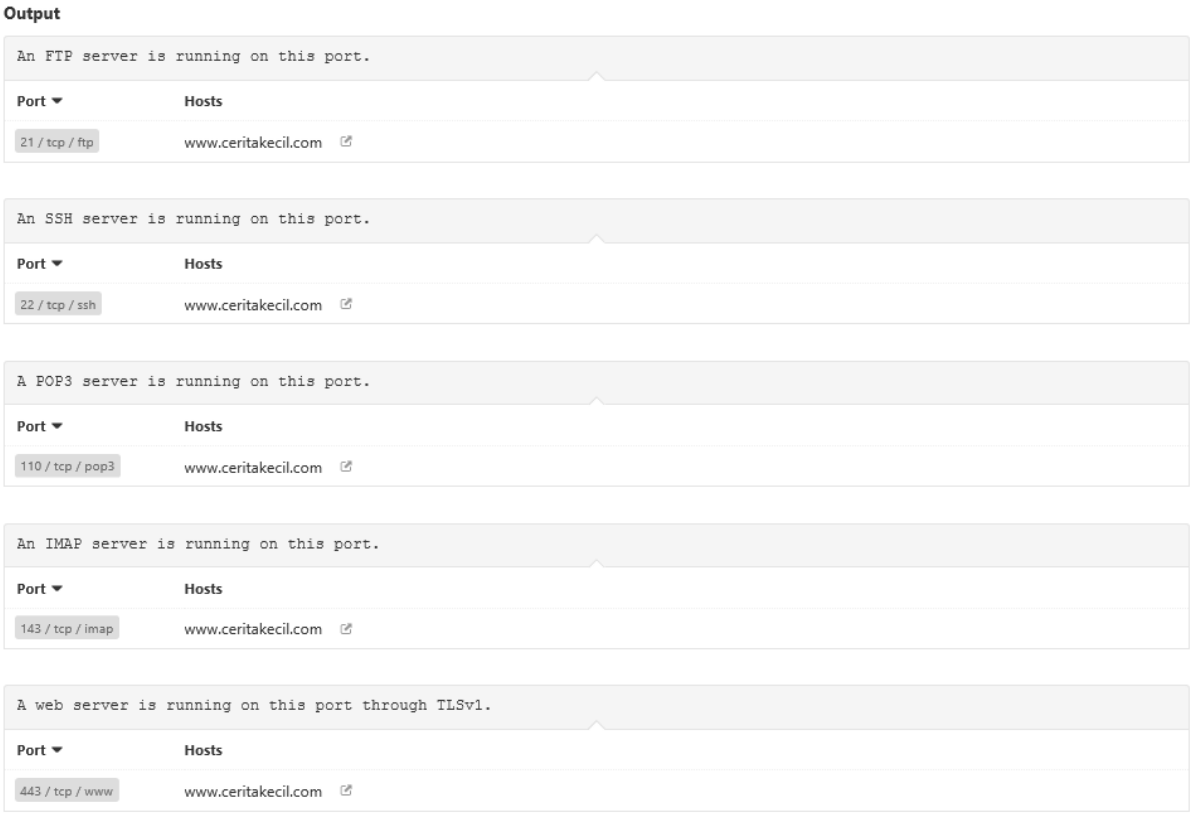


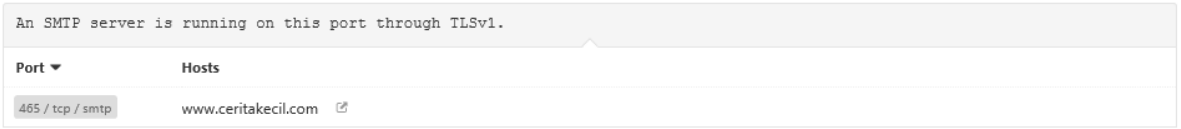
Dari data diatas domain name target www.ceritakecil.com memiliki 19 open port, yaitu:

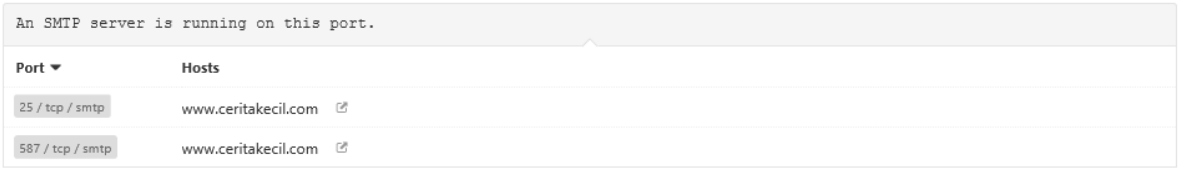
No.	Open Port	Protocol
1	21	tcp
2	22	Tcp
3	25	Tcp
4	53	Tcp
5	80	Tcp
6	110	tcp
7	143	Tcp
8	443	Tcp

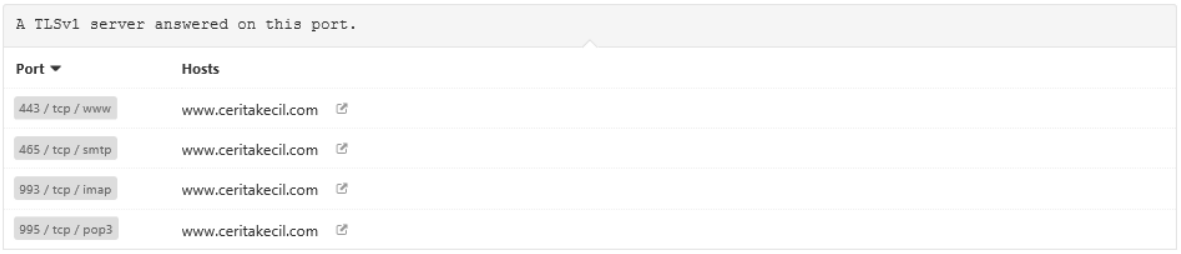
9	465	Tcp
10	587	Tcp
11	993	Tcp
12	995	Tcp
13	2077	Tcp
14	2078	Tcp
15	2082	Tcp
16	2083	Tcp
17	2095	Tcp
18	2096	Tcp
19	8080	Tcp

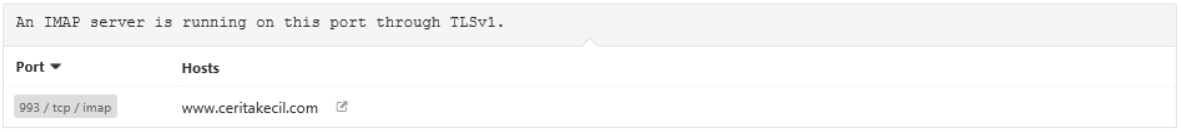
B. Daemon (Service)

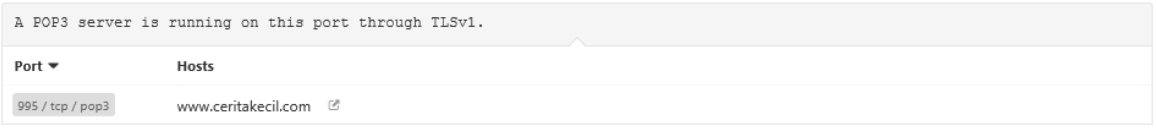


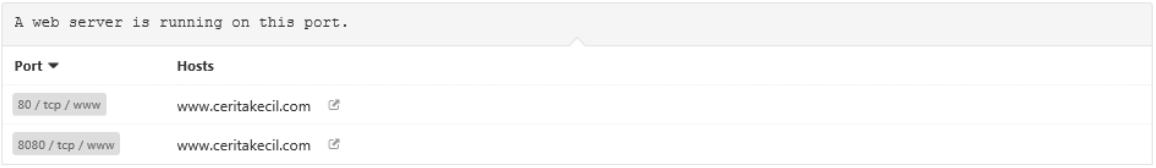












No.	Open Port	Protocol	Service (Daemon)
1	21	tcp	ftp
2	22	Tcp	Ssh
3	110	Tcp	Pop3
4	143	Tcp	Imap
5	443	Tcp	www (web server)
6	465	Tcp	Smtp
7	25	Tcp	Smtp
8	587	Tcp	Smtp
9	443	Tcp	www (web server)
10	465	Tcp	Smtp

11	993	Tcp	Imap
12	995	Tcp	Pop3
13	993	Tcp	Imap
14	995	Tcp	Pop3
15	80	Tcp	www (web server)
16	8080	tcp	www (web server)

C. Vulnerability

Severity ▲	Plugin Name	Plugin Family	Count
HIGH	MTA Open Mail Relaying Allowed	SMTP problems	1
MEDIUM	SSL Certificate with Wrong Hostname	General	4
LOW	SMTP Service Cleartext Login Permitted	SMTP problems	2
LOW	FTP Supports Cleartext Authentication	FTP	1
LOW	POP3 Cleartext Logins Permitted	Misc.	1

Pada vulnerability kali ini hanya memeliki satu rating high pada saverity. Berikut data yang didapat;

HIGH MTA Open Mail Relaying Allowed

Description

The remote SMTP server appears to allow mail relaying. This means that an unauthenticated, remote user could possibly use the mail server to send messages to the world, thus wasting network bandwidth and computer resources. Such servers are targeted by spammers for sending unsolicited bulk email (UBE).

In some scenarios, the number of messages enqueued for delivery could be in the hundreds of thousands, causing the mail server to crash. In addition, SMTP servers that allow relaying are frequently added to real-time block lists maintained by security sites and used by companies world-wide. If added to such a list, delivery of legitimate mail could be severely impacted, causing a form of denial of service.

Solution

Investigate whether the server should allow mail relaying.

If it should not, consult the product documentation or contact the vendor in order to reconfigure the server to reject relaying attempts.

Otherwise, make sure that the service uses appropriate access controls to limit the extent to which relaying is possible.

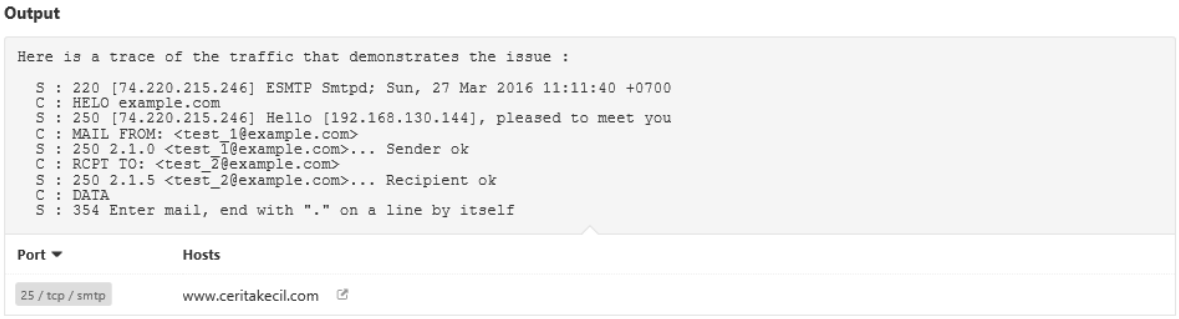
Analisa Deskripsi:

Jadi Remote SMTP server muncul untuk mengizinkan penyiaran email. Berarti pengguna yang tidak berkepentingan dapat menggunakan mail server untuk mengirim email spam sehingga membuang-buang bandwidth jaringan dan sumber daya komputer. Realitanya jumlah pesan menunggu dalam pengiriman pesan dapat mencapai ratusan ribu sehingga menyebabkan mail server crash.

Selain itu juga server smtp memungkinkan pesan tersebut ditambahkan ke daftar real-time blok yang dikelola situs keamanan. Pada kasus seperti ini, pengiriman surat yang sah dapat sangat mempengaruhi sehingga menyebabkan bentuk penolakan layanan.

Analisa Solusi:

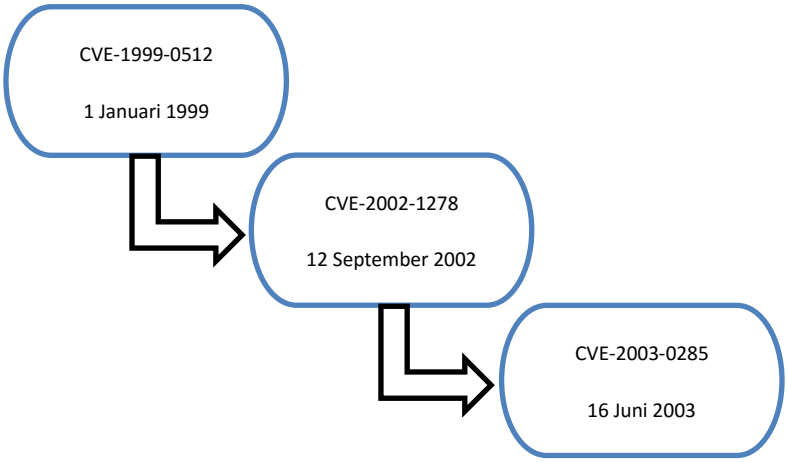
Harus diselidiki apakah server harus memungkinkan penyiaran pesan. Jika tidak boleh, periksa dokumentasi produk atau hubungi vendor untuk mengkonfigurasi server untuk menolak upaya penyiaran pesan. sebaliknya, pastikan bahwa layanan menggunakan kontrol akses yang tepat untuk membatasi sejauh mana kemungkinan peyiaran pesan.



Pada vulnerability dengan severity high terdapat pada port 25, protocol tcp, dan service (daemon) smtp.

D. CVE

Adapun untuk cve mappingnya dibuat seperti ini:



3. Port Scanner

Percobaan ketiga kali ini menggunakan port scanner dengan cara memasukkan ip target yaitu 74.220.215.246

Service	Details
FTP	Pure-FTPd
Port **22** (TCP)	OpenSSH 5.3 protocol 2.0
Port **25** (TCP)	smtp
Port **26** (TCP)	Exim smtpd 4.86_2
Port **53** (TCP)	
Port **110** (TCP)	Dovecot pop3d
Port **143** (TCP)	Dovecot imapd
Port **443** (TCP)	Tunnel is TLSv1: Apache httpd
Port **465** (TCP)	Tunnel is TLSv1: Exim smtpd 4.86_2
Port **587** (TCP)	Exim smtpd 4.86_2
Port **993** (TCP)	Tunnel is TLSv1: Dovecot imapd
Port **995** (TCP)	Tunnel is TLSv1: Dovecot pop3d

Open Port:

No	Open Port	Protocol
1	22	tcp
2	25	Tcp
3	26	Tcp
4	53	Tcp
5	110	Tcp
6	143	Tcp
7	443	Tcp
8	465	tcp
9	587	Tcp
10	993	Tcp
11	995	Tcp

Daemon (Service):

No	Open Port	Daemon (Service)
1	22	Ssh
2	25	Smtp
3	26	Smtp
4	53	
5	110	Pop3
6	143	Imap
7	443	http

8	465	Smtp
9	587	Smtp
10	993	Imap
11	995	Pop3

Untuk Port Scanner ini tidak diketemukan vulnerability dan cve nya.

Daftar Pustaka:

1. www.Nmap.org/Zenmap
2. www.Nessus.org
3. www.advanced-port-scanner.com